Shared Service Provider
Repository Service Requirements
January 23, 2004

This document outlines the requirements vendors must meet in their repository service offering in order to become qualified under the Shared Service Provider (SSP) Program. Tables I, II, and III contain the list of mandatory requirements that must be met by all vendors as a qualified SSP. Table IV contains the list of requirements that must be met by vendors that include end user certificates in their repositories. All requirements were derived from at least one of the following documents: [X509], [RFC2587], [RFC2633], [CCP], [DoD GDS], and [FPKIDIR].

	Table I - Mandatory Repository Service Requirements	Reference
1	The repository service shall contain all the provider's Certificate Authority (CA) certificates except for self-signed certificates	[CCP]
2	The repository service shall contain all Certificate Revocation Lists (CRLs) issued by all the provider's CAs	[CCP]
3	The repository service shall allow unauthenticated access by the public to the information (CA certificates and CRLs) within the directory	[CCP]
4	The scheduled downtime for the repository service shall not exceed .05% per year.	[GDS]
5	The repository service shall provide an average three second response time (or less) from the time the repository receives the request until it delivers the response to the network	[GDS]

	Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements	Reference
1	The repository service shall provide at minimum a Lightweight Directory Access Protocol (LDAP) interface at the port 389, supporting both LDAP versions 2 and 3	[CCP]
2	Directory entries shall use Distinguished Names (DNs) in the form geopolitical names (c=, o=, ou=...) or be constructed using Domain Components (dc=)	[CCP]
3	CA entries shall use at least one of the following as a base object class: *person*, *organizationalPerson*, *inetOrgPerson*, or *organizationalUnit*	[FPKIDIR]

	Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements	Reference
4	CA entries shall include the auxiliary *pkiCA* object class	[FPKIDIR]
5	CA entries shall include the *commonName* or *organizationalUnitName* attribute	[FPKIDIR]
6	c*ACertificate* attribute of a CA's directory entry shall include all certificates issued to the provider's CA; including self-issued certificates	[FPKIDIR]
7	Each CRL issued by the provider's CA(s) shall be stored in the all of the directory entries specified in a distribution point name in the issuingDistributionPoint extension of the CRL.	
8	Each CRL issued by the provider's CA(s) that does not include an issuingDistributionPoint extension or includes an issuingDistributionPoint extension that does not include the distributionPoint field shall be stored in the provider's CA(s) directory entry.	[X509] [RFC2587]
9	Each CRL issued by the provider's CA(s) that includes an issuingDistributionPoint extension with onlyContainsCACerts set to TRUE shall be stored in the authorityRevocationList attribute of the appropriate directory entry or entries.	[X509] [RFC2587]
10	Each CRL issued by the provider's CA(s) that does not include an issuingDistributionPoint extension or includes an issuingDistributionPoint extension with onlyContainsCACerts set to FALSE shall be stored in the certificateRevocationList attribute of the appropriate directory entry or entries.	[X509] [RFC2587]
11	The issuedToThisCA (forward) elements of the *crossCertificatePair* attribute of a CA's directory entry shall be used to store all certificates, except self-issued certificates, issued to the provider's CA.	[X509] [RFC2587]
12	The issuedByThisCA (reverse) elements of the *crossCertificatePair* attribute of a CA's directory entry shall contain all certificates issued by the provider's CA to other CAs.	[X509] [RFC2587]
13	When both the issuedToThisCA (forward) and issuedByThisCA (reverse) elements of the *crossCertificatePair* attribute are present in a single attribute value of a CA's directory entry, the issuer name in one certificate shall match the subject name in the other and vice versa.	[X509] [RFC2587]
14	When both the issuedToThisCA (forward) and issuedByThisCA (reverse) elements of the *crossCertificatePair* attribute are present in a single attribute value of a CA's directory entry, the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.	[X509] [RFC2587]

	Table III - Mandatory Repository Service Hyper Text Transmission Protocol (HTTP) Access Requirements	Reference
1	The repository service shall provide at minimum a Hyper Text Transmission Protocol (HTTP) version 1.1 interface at the port 80	
2	CRLs issued by the provider's CA shall be stored in files with a .crl extension. The files shall contain the DER-encoded CRL.	[RFC2633]
3	CA certificates issued to the provider's CA shall be stored as a degenerate *signedData* "certs-only" message in a file with a .p7c extension. (This includes self-issued certificates.)	[RFC2633]
4	CA certificates issued by the provider's CA shall be stored as a degenerate *signedData* "certs-only" message in a file with a .p7c extension. (This includes self-issued certificates.)	[RFC2633]

	Table IV – End Entity Certificate Repository Service Requirements	Reference
1	End Entity entries shall use one of the following classes: *person* OR *device*	[FPKIDIR]
2	End Entity entries shall use *pkiUser* class	[FPKIDIR]
3	The *userCertificate* attribute of an End Entity's directory entry shall include all certificates issued to End Entity by the provider's CA(s)	[FPKIDIR]

References:

[X509] - ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: 1997, "Information technology - Open Systems Interconnection - The Directory: Authentication framework", June 1997.

[RFC2587] - Boeyen, S., Howes, T., and P. Richard, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", RFC2587, June 1999.

[RFC2633] - B. Ramsdell, "S/MIME Version 3 Message Specification", RFC2633, June 1999.

[FPKIDIR] - Federal Public Key Infrastructure, Directory Profile, October 8, 2002.

[CCP] - X.509 Certificate Policy for the Common Policy Framework, May 8, 2003.

[GDS] - "GLOBAL DIRECTORY SERVICE: Requirements Identification Document", Version 1.0, 4 September 2001.